

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of :  
Yuichi FUTA et al. :  
Serial No. NEW : **Attn: APPLICATION BRANCH**  
Filed April 13, 2004 : Attorney Docket No. 2004\_0582A  
APPARATUS AUTHENTICATION :  
SYSTEM, SERVER APPARATUS, AND  
CLIENT APPARATUS :

**CLAIM OF PRIORITY UNDER 35 USC 119**

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

THE COMMISSIONER IS AUTHORIZED  
TO CHARGE ANY DEFICIENCY IN THE  
FEES FOR THIS PAPER TO DEPOSIT  
ACCOUNT NO. 23-0975

Sir:

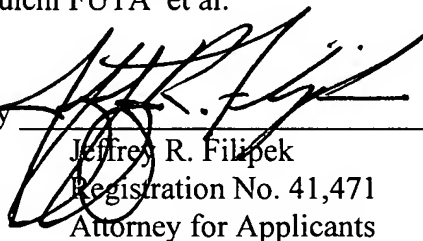
Applicants in the above-entitled application hereby claim the date of priority under the International Convention of Japanese Patent Application No. 2003-109264, filed April 14, 2003, as acknowledged in the Declaration of this application.

A certified copy of said Japanese Patent Application is submitted herewith.

Respectfully submitted,

Yuichi FUTA et al.

By

  
Jeffrey R. Filipek  
Registration No. 41,471  
Attorney for Applicants

JRF/fs  
Washington, D.C. 20006-1021  
Telephone (202) 721-8200  
Facsimile (202) 721-8250  
April 13, 2004

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日                      2 0 0 3 年    4 月 1 4 日  
Date of Application:

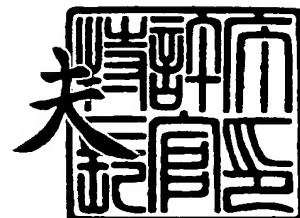
出 願 番 号                      特 願 2 0 0 3 - 1 0 9 2 6 4  
Application Number:  
[ST. 10/C] :                      [ J P 2 0 0 3 - 1 0 9 2 6 4 ]

出      願      人                      松下電器産業株式会社  
Applicant(s):

2 0 0 4 年    2 月 1 0 日

特許庁長官  
Commissioner,  
Japan Patent Office

今 井 康 夫



【書類名】 特許願

【整理番号】 2022550157

【提出日】 平成15年 4月14日

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 12/14

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 布田 裕一

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 松崎 なつめ

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 山内 弘貴

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 太田 雄策

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 臼木 直司

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 綾木 靖

**【発明者】**

**【住所又は居所】** 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

**【氏名】** 森岡 芳宏

**【特許出願人】**

**【識別番号】** 000005821

**【氏名又は名称】** 松下電器産業株式会社

**【代理人】**

**【識別番号】** 100090446

**【弁理士】**

**【氏名又は名称】** 中島 司朗

**【手数料の表示】**

**【予納台帳番号】** 014823

**【納付金額】** 21,000円

**【提出物件の目録】**

**【物件名】** 明細書 1

**【物件名】** 図面 1

**【物件名】** 要約書 1

**【包括委任状番号】** 9003742

**【プルーフの要否】** 要

【書類名】 明細書

【発明の名称】 機器認証システム、機器認証装置、機器認証方法及び記録媒体

【特許請求の範囲】

【請求項 1】 第 1 のネットワークに接続しているサーバにより第 2 のネットワークに接続している機器を認証する機器認証システムであって、

前記サーバは、チャレンジデータを作成し、前記機器へ送信するチャレンジ送信手段と、

署名データを受信する署名受信手段と、

前記署名データが、前記チャレンジデータと前記サーバに予め設定されている第 1 のパスワードデータに基づく第 1 の署名対象データに対する正しい署名であるか否かを検証する署名検証手段を備え、

前記機器は、前記チャレンジデータを受信するチャレンジ受信手段と、

前記チャレンジデータと、前記機器に予め設定されている第 2 のパスワードデータに基づく第 2 の署名対象データを作成する署名対象データ作成手段と、

前記第 2 の署名対象データに対する前記署名データを作成する署名作成手段と

前記署名データを送信する署名送信手段を備える

ことを特徴とする機器認証システム。

【請求項 2】 前記第 2 のパスワードデータは、外部から入力されることを特徴とする請求項 1 記載の機器認証システム。

【請求項 3】 前記機器は、さらに外部より入力された第 3 のパスワードデータを前記第 2 のパスワードデータに登録するパスワード登録手段を備えることを特徴とする請求項 1 記載の機器認証システム。

【請求項 4】 前記機器は、さらにネットワークを介して前記第 3 のパスワードデータを受信するパスワード受信手段と、

前記第 3 のパスワードデータが送信されたパスワード送信元が前記第 2 のネットワークに接続しているか否かを判定するパスワード送信元判定手段を備え、

前記パスワード登録手段は、前記パスワード送信元が前記第 2 のネットワークに接続していると判定された場合のみに、前記第 3 のパスワードデータを前記第

2 のパスワードデータに登録する

ことを特徴とする請求項 3 記載の機器認証システム。

【請求項 5】前記機器は、さらに前記第 3 のパスワードデータの長さを計測し、前記第 3 のパスワードデータの長さが予め与えられた値以上であるか否かを判定するデータ長判定部を備え、

前記パスワード登録手段は、前記第 3 のパスワードデータの長さが予め与えられた値以上である場合に、前記第 3 のパスワードデータを前記第 2 のパスワードデータに登録する

ことを特徴とする請求項 3 記載の機器認証システム。

【請求項 6】前記サーバは、さらに前記第 2 のネットワークが前記第 1 のネットワークと同一であることを判定するネットワーク判定手段を備え、

前記署名検証手段は、前記判定が肯定的である場合、前記署名データが前記チャレンジデータと前記サーバに予め設定されている第 4 のパスワードデータに基づく第 3 の署名対象データに対する正しい署名であるか否かを検証し、否定的である場合、前記前記署名データが前記チャレンジデータと前記サーバに予め設定されている第 5 のパスワードデータに基づく第 4 の署名対象データに対する正しい署名であるか否かを検証する

ことを特徴とする請求項 1 から請求項 4 のいずれか 1 項に記載の機器認証システム。

【請求項 7】前記署名生成手段及び前記署名検証手段で使用する署名方法は公開鍵署名方法であることを特徴とする請求項 1 から請求項 6 のいずれか 1 項に記載の機器認証システム。

【請求項 8】前記署名生成手段及び前記署名検証手段で使用する署名方法は鍵付ハッシュ関数を利用することを特徴とする請求項 1 から請求項 6 のいずれか 1 項に記載の機器認証システム。

【請求項 9】機器を認証する機器認証装置であって、

チャレンジデータを作成し、前記機器へ送信するチャレンジ送信部と、

署名データを受信する署名受信部と、

前記署名データが、前記チャレンジデータと予め設定されている第 1 のパスワ

ードデータに基づく第1の署名対象データに対する正しい署名であるか否かを検証する署名検証手段を備える

ことを特徴とする機器認証装置。

【請求項10】さらに前記機器が接続している第2のネットワークが前記機器認証装置が接続している第1のネットワークと同一であることを判定するネットワーク判定手段を備え、

前記署名検証手段は、前記判定が肯定的である場合、前記前記署名データが前記チャレンジデータと前記サーバに予め設定されている第4のパスワードデータに基づく第3の署名対象データに対する正しい署名であるか否かを検証し、否定的である場合、前記前記署名データが前記チャレンジデータと前記サーバに予め設定されている第5のパスワードデータに基づく第4の署名対象データに対する正しい署名であるか否かを検証する

ことを特徴とする請求項9記載の機器認証装置。

【請求項11】第1のネットワークに接続しているサーバにより第2のネットワークに接続している機器を認証する機器認証方法であって、

前記サーバにより、チャレンジデータを作成し、前記機器へ送信するチャレンジ送信ステップと、

前記機器により、前記チャレンジデータを受信するチャレンジ受信ステップと

、  
前記機器により、前記チャレンジデータと、前記機器に予め設定されている第2のパスワードデータに基づく第2の署名対象データを作成する署名対象データ作成ステップと、

前記機器により、前記第2の署名対象データに対する署名データを作成する署名作成ステップと、

前記機器により、前記署名データを送信する署名送信ステップと、

前記サーバにより、署名データを受信する署名受信ステップと、

前記サーバにより、前記署名データが、前記チャレンジデータと前記サーバに予め設定されている第1のパスワードデータに基づく第1の署名対象データに対する正しい署名であるか否かを検証する署名検証ステップを含む

ことを特徴とする機器認証方法。

【請求項 1 2】さらに、前記機器により、外部より入力された第 3 のパスワードデータを前記第 2 のパスワードデータに登録するパスワード登録ステップを含むことを特徴とする請求項 1 1 記載の機器認証方法。

【請求項 1 3】さらに、前記機器により、ネットワークを介して前記第 3 のパスワードデータを受信するパスワード受信ステップと、

前記機器により、前記第 3 のパスワードデータが送信されたパスワード送信元が前記第 2 のネットワークに接続しているか否かを判定するパスワード送信元判定ステップを含み、

前記パスワード登録ステップは、前記機器により、前記パスワード送信元が前記第 2 のネットワークに接続していると判定された場合のみに、前記第 3 のパスワードデータを前記第 2 のパスワードデータに登録する

ことを特徴とする請求項 1 1 記載の機器認証方法。

【請求項 1 4】さらに、前記サーバにより、前記第 2 のネットワークが前記第 1 のネットワークと同一であることを判定するネットワーク判定ステップを含み、

前記署名検証ステップは、前記サーバにより、前記判定が肯定的である場合、前記前記署名データが前記チャレンジデータと前記サーバに予め設定されている第 4 のパスワードデータに基づく第 3 の署名対象データに対する正しい署名であるか否かを検証し、否定的である場合、前記前記署名データが前記チャレンジデータと前記サーバに予め設定されている第 5 のパスワードデータに基づく第 4 の署名対象データに対する正しい署名であるか否かを検証する

ことを特徴とする請求項 1 1 から請求項 1 3 のいずれか 1 項に記載の機器認証方法。

【請求項 1 5】第 1 のネットワークに接続しているサーバにより第 2 のネットワークに接続している機器を認証する処理をコンピュータに実行させるプログラムを記録したコンピュータ読取可能な記録媒体であって、

前記サーバにより、チャレンジデータを作成し、前記機器へ送信するチャレンジ送信ステップと、



前記機器により、前記チャレンジデータを受信するチャレンジ受信ステップと

前記機器により、前記チャレンジデータと、前記機器に予め設定されている第2のパスワードデータに基づく第2の署名対象データを作成する署名対象データ作成ステップと、

前記機器により、前記第2の署名対象データに対する署名データを作成する署名作成ステップと、

前記機器により、前記署名データを送信する署名送信ステップと、

前記サーバにより、署名データを受信する署名受信ステップと、

前記サーバにより、前記署名データが、前記チャレンジデータと前記サーバに予め設定されている第1のパスワードデータに基づく第1の署名対象連結データに対する正しい署名であるか否かを検証する署名検証ステップと

をコンピュータに実行させることを特徴とするプログラムを記録したコンピュータ読取可能な記録媒体。

【請求項16】さらに、前記機器により、外部より入力された第3のパスワードデータを前記第2のパスワードデータに登録するパスワード登録ステップ

をコンピュータに実行させることを特徴とするプログラムを記録した請求項15記載のコンピュータ読取可能な記録媒体。

【請求項17】さらに、前記機器により、ネットワークを介して前記第3のパスワードデータを受信するパスワード受信ステップと、

前記機器により、前記第3のパスワードデータが送信されたパスワード送信元が前記第2のネットワークに接続しているか否かを判定するパスワード送信元判定ステップをコンピュータに実行させ、

前記パスワード登録ステップは、前記機器により、前記パスワード送信元が前記第2のネットワークに接続していると判定された場合のみに、前記第3のパスワードデータを前記第2のパスワードデータに登録する

ことを特徴とするプログラムを記録した請求項16記載のコンピュータ読取可能な記録媒体。

【請求項18】さらに、前記サーバにより、前記第2のネットワークが前記第

1のネットワークと同一であることを判定するネットワーク判定ステップをコンピュータに実行させ、

前記署名検証ステップは、前記サーバにより、前記判定が肯定的である場合、前記前記署名データが前記チャレンジデータと前記サーバに予め設定されている第4のパスワードデータに基づく第3の署名対象データに対する正しい署名であるか否かを検証し、否定的である場合、前記前記署名データが前記チャレンジデータと前記サーバに予め設定されている第5のパスワードデータに基づく第4の署名対象データに対する正しい署名であるか否かを検証する

ことを特徴とするプログラムを記録した請求項15から請求項17のいずれか1項に記載のコンピュータ読取可能な記録媒体。

#### 【発明の詳細な説明】

##### 【0001】

#### 【発明の属する技術分野】

本発明は、機器認証システム、機器認証装置、機器認証方法及び記録媒体に関し、特にパスワード認証を機器認証に組み合わせることによりコンテンツの著作権保護を図りつつ、実装上の負荷を軽減する技術に関する。

##### 【0002】

#### 【従来の技術】

近年、音楽や映像、ゲームなどデジタルコンテンツはインターネットやデジタル放送および、パッケージメディアによる流通により容易に取得が可能となってきた。

このようなシステムでは、通常、コンテンツの著作権を保護するために、コンテンツは暗号化され、それを獲得する権利のある機器だけが復号できるようになっている。例えば、インターネットを用いたデジタルコンテンツの配布では、配布元であるサーバと、コンテンツを利用するクライアント機器の間で認証が行われ、サーバは予め登録されたクライアント機器であることを確認後、コンテンツをそのクライアント機器だけが有する鍵を用いて暗号化して配布する。

##### 【0003】

以下に、サーバとクライアント機器間の認証方法の一例として、公開鍵暗号を

用いた相手認証方法を示す（例えば、非特許文献1参照）。

第1の機器が第2の機器にチャレンジデータとして乱数データを送信し、続いて、第2の機器がその乱数データに対して自分の秘密鍵で暗号化（電子署名など）して第1の機器にレスポンスデータを返信し、最後に、返信されてきた暗号文（あるいは、署名文）に対して、第1の機器が第2の機器の公開鍵を用いて検証するというものがある。一般に、このような公開鍵暗号を用いた認証においては、公開鍵そのものが有効であることが前提となる。

#### 【0004】

このために、認証局と呼ばれる機関から、各機器に対応する正しい公開鍵であることを示す（公開鍵に対する「お墨付き」となる）「公開鍵証明書」が発行されることが一般的である。公開鍵証明書は、機器の識別名や有効期限と公開鍵を結合したデータに認証局の電子署名が付与されたものであり、これを受け取った機器は、その電子署名の正しさを確認し、さらに通信機器の識別名や現在の時間からその公開鍵証明書の記載内容を確認した上で、公開鍵の正しさを確認するのである。さらに、発行された公開鍵証明書のうち、不正を働いた機器、あるいは秘密鍵が盗まれた機器の公開鍵証明書については、それらが無効化されていることを他の機器に知らせるために、無効化した公開鍵証明書を特定する情報の一覧に対して認証局の電子署名が付与された公開鍵証明書無効化リスト（Certificate Revocation List：以下、CRL）として発行される（例えば、非特許文献2参照）。

#### 【0005】

このように、相手機器の公開鍵を用いてその相手機器を認証する際には、その相手機器から公開鍵証明書入手し、入手した公開鍵証明書がCRLに登録されたもの（無効化されたもの）でないことを確認する。

一方、高速シリアルバス規格の1つのIEEE1394を介して配信されるデジタルコンテンツの保護規格として、DTCP（Digital Transmission Content Protection）と呼ばれる規格がある（例えば、非特許文献3参照）。

#### 【0006】

D T C Pでは、D T L A (D i g i t a l T r a n s m i s s i o n L i c e n s i n g A d m i n i s t r a t o r、L L C) と呼ばれる管理者の管理の下でD T C P規格に準拠した機器を相互接続し、その間で暗号認証通信を行っている。その仕組みの概要は次の通りである。

(1) 送信機器および受信機器は、それぞれD T L Aから配布された秘密鍵と証明書を備えている。この秘密鍵と証明書の配布はD T L Aとの契約に基づいて各機器に配布される。

#### 【0007】

(2) 送信機器と受信機器は、上記秘密鍵を用いて相互認証する。また、送信機器は、著作権保護が必要となるコンテンツを、認証により共有した鍵で暗号化して送信する。なお、鍵の共有方法はディフィーヘルマン (D H) 鍵共有方法 (例えば非特許文献4) をベースにして楕円曲線暗号上にD T C P規格で独自に規定されたものである。

#### 【0008】

ところで、上記D T C Pコンテンツ保護の仕組みを無線通信の世界まで拡張することを考えた場合、I E E E 1394のような有線バスと異なり、盗聴やなりすましなどの攻撃が容易であることが懸念される。例えば近くを通りかかった受信機器がD T L Aから配布された秘密鍵を持ってさえいれば、他人の機器が許可無く勝手に接続する危険がある。このことは著作権保護の観点から言って問題である。また、その送信機器を保有する個人がどのようなコンテンツに興味があるのかが暴露する可能性もあり、プライバシー保護の点でも問題がある。

#### 【0009】

この問題を解決する1つの方法として、無線のセキュリティ機能、例えばI E E E 802.11bで決められているW E P (W i r e d E q u i v a l e n t P r i v a c y、例えば非特許文献5) を、上記認証に加えて使用することが考えられる。ユーザはパスワードを予めアクセスポイントに設定し、同じパスワードを機器側に入力しないと接続できない。つまり、パスワードを知らない他人が勝手に接続する危険はなくなる。具体的にはパスワードを用いて、チャレンジデータに対するレスポンスを生成し、これにより認証を行う。さらに、パスワ

ードを用いて通信データのMAC層での暗号化を行っている。

【0 0 1 0】

【非特許文献1】

岡本龍明、山本博資、”現代暗号”、産業図書（1997年）、155ページ～156ページ

【0 0 1 1】

【非特許文献2】

American National Standards Institute, American National Standard for Financial Services, ANSX9.57: Public Key Cryptography For the Financial Industry: Certificate Management, 1997.

【0 0 1 2】

【非特許文献3】

D T C P   S p e c i f i c a t i o n の W h i t e   p a p e r   < U R L :   H Y P E R L I N K   ” <http://www.dtcp.com/spec.html> ” <http://www.dtcp.com/spec.html> >

【0 0 1 3】

【非特許文献4】

池野信一、小山謙二、「現代暗号理論」、電子通信学会、175ページ～177ページ

【0 0 1 4】

【非特許文献5】

W E P 暗号化の基礎と実践 < U R L :   H Y P E R L I N K   ” <http://www.atmarkit.co.jp/fwin2k/operation/wirelesswep/wirelesswep01.html> ” <http://www.atmarkit.co.jp/fwin2k/operation/wirelesswep/wirelesswep01.html> >

【0 0 1 5】

【発明が解決しようとする課題】

上記述べたD T C P に W E P を組み合わせた方法では、アクセスポイントのW E P を O N にする／しないの選択はユーザ任せである。そのためプライバシーの問題はユーザの責任なのでしかたがないが、コンテンツ著作権保護の観点からは

問題である。また、認証部分では D T C P の認証と W E P の認証の双方が個別に必要であり、送信機器と受信機器の間のトランザクションが多くなる。さらに、D T C P はアプリケーション層でコンテンツの暗号化を行い、さらに W E P では M A C 層での通信データの暗号化を行うため、送信機器および受信機器においてもその負荷は大きい。2重で暗号化するのも無駄である。以上述べたとおり、実装上の観点から課題がある。

#### 【0016】

本発明では、パスワード認証を D T C P のような機器認証に組み合わせることにより、コンテンツ著作権保護の課題を解決し、さらに実装上也負荷にならない方法を実現する。

#### 【0017】

##### 【課題を解決するための手段】

上記課題を解決するために、請求項1における機器認証システムは、第1のネットワークに接続しているサーバにより第2のネットワークに接続している機器を認証する機器認証システムであって、前記サーバは、チャレンジデータを作成し、前記機器へ送信するチャレンジ送信手段と、署名データを受信する署名受信手段と、前記署名データが、前記チャレンジデータと前記サーバに予め設定されている第1のパスワードデータに基づく第1の署名対象データに対する正しい署名であるか否かを検証する署名検証手段を備え、前記機器は、前記チャレンジデータを受信するチャレンジ受信手段と、前記チャレンジデータと、前記機器に予め設定されている第2のパスワードデータに基づく第2の署名対象データを作成する署名対象データ作成手段と、前記第2の署名対象データに対する前記署名データを作成する署名作成手段と、前記署名データを送信する署名送信手段を備える。

#### 【0018】

請求項2における機器認証システムは、請求項1における前記第2のパスワードデータが、外部から入力されることを特徴とする。

請求項3における機器認証システムは、請求項1の前記機器は、さらに外部より入力された第3のパスワードデータを前記第2のパスワードデータに登録する

パスワード登録手段を備えることを特徴とする。

【0019】

請求項4における機器認証システムは、請求項3における前記機器は、さらにネットワークを介して前記第3のパスワードデータを受信するパスワード受信手段と、前記第3のパスワードデータが送信されたパスワード送信元が前記第2のネットワークに接続しているか否かを判定するパスワード送信元判定手段を備え、

前記パスワード登録手段は、前記パスワード送信元が前記第2のネットワークに接続していると判定された場合のみに、前記第3のパスワードデータを前記第2のパスワードデータに登録することを特徴とする。

【0020】

請求項5における機器認証システムは、請求項3における前記機器は、さらに前記第3のパスワードデータの長さを計測し、前記第3のパスワードデータの長さが予め与えられた値以上であるか否かを判定するデータ長判定部を備え、前記パスワード登録手段は、前記第3のパスワードデータの長さが予め与えられた値以上である場合に、前記第3のパスワードデータを前記第2のパスワードデータに登録することを特徴とする。

【0021】

請求項6における機器認証システムは、請求項1から請求項4のいずれかの1項における前記サーバは、さらに前記第2のネットワークが前記第1のネットワークと同一であることを判定するネットワーク判定手段を備え、前記署名検証手段は、前記判定が肯定的である場合、前記署名データが前記チャレンジデータと前記サーバに予め設定されている第4のパスワードデータに基づく第3の署名対象データに対する正しい署名であるか否かを検証し、否定的である場合、前記前記署名データが前記チャレンジデータと前記サーバに予め設定されている第5のパスワードデータに基づく第4の署名対象データに対する正しい署名であるか否かを検証することを特徴とする。

【0022】

請求項7における機器認証システムは、請求項1から請求項6のいずれか1項

における前記署名生成手段及び前記署名検証手段で使用する署名方法は公開鍵署名方法であることを特徴とする。

請求項 8 における機器認証システムは、請求項 1 から請求項 6 のいずれか 1 項における前記署名生成手段及び前記署名検証手段で使用する署名方法は鍵付ハッシュ関数を利用することを特徴とする。

#### 【 0 0 2 3 】

請求項 9 における機器認証装置は、チャレンジデータを作成し、前記機器へ送信するチャレンジ送信部と、署名データを受信する署名受信部と、前記署名データが、前記チャレンジデータと予め設定されている第 1 のパスワードデータに基づく第 1 の署名対象データに対する正しい署名であるか否かを検証する署名検証手段を備える。

#### 【 0 0 2 4 】

請求項 1 0 における機器認証装置は、請求項 9 にさらに前記機器が接続している第 2 のネットワークが前記機器認証装置が接続している第 1 のネットワークと同一であることを判定するネットワーク判定手段を備え、前記署名検証手段は、前記判定が肯定的である場合、前記前記署名データが前記チャレンジデータと前記サーバに予め設定されている第 4 のパスワードデータに基づく第 3 の署名対象データに対する正しい署名であるか否かを検証し、否定的である場合、前記前記署名データが前記チャレンジデータと前記サーバに予め設定されている第 5 のパスワードデータに基づく第 4 の署名対象データに対する正しい署名であるか否かを検証することを特徴とする。

#### 【 0 0 2 5 】

請求項 1 1 における機器認証方法は、第 1 のネットワークに接続しているサーバにより第 2 のネットワークに接続している機器を認証する機器認証方法であって、前記サーバにより、チャレンジデータを作成し、前記機器へ送信するチャレンジ送信ステップと、前記機器により、前記チャレンジデータを受信するチャレンジ受信ステップと、前記機器により、前記チャレンジデータと、前記機器に予め設定されている第 2 のパスワードデータに基づく第 2 の署名対象データを作成する署名対象データ作成ステップと、前記機器により、前記第 2 の署名対象デー



タに対する署名データを作成する署名作成ステップと、前記機器により、前記署名データを送信する署名送信ステップと、前記サーバにより、署名データを受信する署名受信ステップと、前記サーバにより、前記署名データが、前記チャレンジデータと前記サーバに予め設定されている第1のパスワードデータに基づく第1の署名対象データに対する正しい署名であるか否かを検証する署名検証ステップを含むことを特徴とする。

#### 【0026】

請求項12における機器認証方法は、請求項11にさらに、前記機器により、外部より入力された第3のパスワードデータを前記第2のパスワードデータに登録するパスワード登録ステップを含むことを特徴とする。

請求項13における機器認証方法は、請求項11にさらに、前記機器により、ネットワークを介して前記第3のパスワードデータを受信するパスワード受信ステップと、前記機器により、前記第3のパスワードデータが送信されたパスワード送信元が前記第2のネットワークに接続しているか否かを判定するパスワード送信元判定ステップを含み、前記パスワード登録ステップは、前記機器により、前記パスワード送信元が前記第2のネットワークに接続していると判定された場合のみに、前記第3のパスワードデータを前記第2のパスワードデータに登録することを特徴とする。

#### 【0027】

請求項14における機器認証方法は、請求項11から請求項13にさらに、前記サーバにより、前記第2のネットワークが前記第1のネットワークと同一であることを判定するネットワーク判定ステップを含み、前記署名検証ステップは、前記サーバにより、前記判定が肯定的である場合、前記前記署名データが前記チャレンジデータと前記サーバに予め設定されている第4のパスワードデータに基づく第3の署名対象データに対する正しい署名であるか否かを検証し、否定的である場合、前記前記署名データが前記チャレンジデータと前記サーバに予め設定されている第5のパスワードデータに基づく第4の署名対象データに対する正しい署名であるか否かを検証することを特徴とする。

#### 【0028】

請求項 15 における記録媒体は、第 1 のネットワークに接続しているサーバにより第 2 のネットワークに接続している機器を認証する処理をコンピュータに実行させるプログラムを記録したコンピュータ読取可能な記録媒体であって、前記サーバにより、チャレンジデータを作成し、前記機器へ送信するチャレンジ送信ステップと、前記機器により、前記チャレンジデータを受信するチャレンジ受信ステップと、前記機器により、前記チャレンジデータと、前記機器に予め設定されている第 2 のパスワードデータに基づく第 2 の署名対象データを作成する署名対象データ作成ステップと、前記機器により、前記第 2 の署名対象データに対する署名データを作成する署名作成ステップと、前記機器により、前記署名データを送信する署名送信ステップと、前記サーバにより、署名データを受信する署名受信ステップと、前記サーバにより、前記署名データが、前記チャレンジデータと前記サーバに予め設定されている第 1 のパスワードデータに基づく第 1 の署名対象データに対する正しい署名であるか否かを検証する署名検証ステップとをコンピュータに実行させることを特徴とする。

#### 【0029】

請求項 16 における記録媒体は、請求項 15 にさらに、前記機器により、外部より入力された第 3 のパスワードデータを前記第 2 のパスワードデータに登録するパスワード登録ステップをコンピュータに実行させることを特徴とする。

請求項 17 における記録媒体は、請求項 16 にさらに、前記機器により、ネットワークを介して前記第 3 のパスワードデータを受信するパスワード受信ステップと、前記機器により、前記第 3 のパスワードデータが送信されたパスワード送信元が前記第 2 のネットワークに接続しているか否かを判定するパスワード送信元判定ステップをコンピュータに実行させ、前記パスワード登録ステップは、前記機器により、前記パスワード送信元が前記第 2 のネットワークに接続していると判定された場合のみに、前記第 3 のパスワードデータを前記第 2 のパスワードデータに登録することを特徴とする。

#### 【0030】

請求項 18 における記録媒体は、請求項 15 から 17 にさらに、前記サーバにより、前記第 2 のネットワークが前記第 1 のネットワークと同一であることを判

定するネットワーク判定ステップをコンピュータに実行させ、前記署名検証ステップは、前記サーバにより、前記判定が肯定的である場合、前記前記署名データが前記チャレンジデータと前記サーバに予め設定されている第4のパスワードデータに基づく第3の署名対象データに対する正しい署名であるか否かを検証し、否定的である場合、前記前記署名データが前記チャレンジデータと前記サーバに予め設定されている第5のパスワードデータに基づく第4の署名対象データに対する正しい署名であるか否かを検証することを特徴とする。

### 【0031】

#### 【発明の実施の形態】

#### 【実施の形態1】

#### 【実施の形態1の構成】

図1は、実施の形態1における、サーバ機器100とクライアント機器101の内部構成を示している。以降、サーバ機器100を単にサーバ、クライアント機器101を単にクライアントとも呼ぶ。

### 【0032】

サーバ機器100は、公開鍵暗号系における公開鍵に信頼できる第3者機関（CA: Certification Authority と呼ぶ）の署名が付与された公開鍵証明書を格納する公開鍵証明書格納部103と、前記公開鍵に対応する秘密鍵を格納する秘密鍵格納部102と、公開鍵暗号の各種処理（署名生成／検証など）を実行する公開鍵暗号処理部104と、登録したパスワードをクライアント機器101固有の識別子と対応付けて格納するパスワード記録部105と、クライアント機器101からの応答を用いてクライアント機器101が正しい機器であり、さらにパスワードが正しいことを認証する認証部106と、クライアント機器101との間で通信を行う入出力部107からなる。

### 【0033】

一方、クライアント機器101は、公開鍵暗号系における公開鍵にCAの署名が付与された公開鍵証明書を格納する公開鍵証明書格納部108と、前記公開鍵に対応する秘密鍵を格納する秘密鍵格納部109と、公開鍵暗号の各種処理（署名生成／検証など）を実行する公開鍵暗号処理部110と、クライアント機器1

01固有の識別子を格納する識別子格納部111と、ユーザのパスワードを入力を受け付けるパスワード入力部112と、サーバ機器100との間で通信を行う入出力部113を備える。

#### 【0034】

ここで、少なくとも、サーバ機器100およびクライアント機器101における秘密鍵格納部102、109、サーバ機器100におけるパスワード記録部105は、例えば耐タンパ領域に格納されて、外部に漏れることなく内部で厳重に管理されるものとする。

#### [実施の形態1のパスワードと機器認証フロー]

図2は、図1におけるサーバ機器100が、クライアント機器101の機器認証およびそれに入力されたパスワードの認証を行う際の動作フローを示している。以下、その詳細について説明する。なお、この動作フローはD T C Pの機器認証にパスワード認証機能を追加しつつ、トランザクションの数および、サーバ機器100とクライアント機器101における計算量は増加しない。

#### 【0035】

S200：ユーザはクライアント機器101にパスワードPWを入力する。具体的には、クライアント機器101におけるパスワード入力部112は、ユーザからパスワードPWを受け付ける。

S201：クライアント機器101はサーバ機器100に対し、公開鍵暗号処理部110で生成した乱数 $r_b$ と、識別子格納部111内に格納されている自身の機器識別子であるID $b$ と、公開鍵証明書格納部108内に格納されている証明書C e r t  $b$ を添えて、認証の要求を行う。

#### 【0036】

S202：サーバ機器100はクライアント機器101の証明書の正しさを確認する。D T C Pでは証明書には楕円曲線暗号の署名方法であるE C - D S Aを用いたC Aの署名が含まれている。この署名をC Aの公開鍵を用いて検証する。

S203：サーバ機器100は、公開鍵暗号処理部104で生成した乱数 $r_a$ と、公開鍵証明書格納部103内に格納されている証明書C e r t  $a$ をクライアント機器101に送付する。

## 【0037】

S204：クライアント機器101は公開鍵暗号処理部110において、サーバ機器100の証明書C e r t aの正しさを確認する。

S205、S206：サーバ機器100およびクライアント機器101それぞれにおいて、楕円曲線暗号のDH鍵共有方法であるEC-DHを用いた初期値X a、X bを計算する。

## 【0038】

S207：サーバ機器100の公開鍵暗号処理部104は、乱数r bをチャレンジデータとして、これに対応した署名応答[A]を生成し、前記X aとともに、クライアント機器101に送付する。署名応答は例えば、r bとX aを連結した情報に対してサーバの秘密鍵を用いて生成する。

S208：クライアント機器101の公開鍵暗号処理部110は、乱数r aをチャレンジデータとし、S200で入力したPWを用いて署名応答[B]を生成し、前記X bとともに、サーバ機器100に送付する。署名応答は例えば、r aとX bおよび、PWを連結した情報に対してクライアント機器101の秘密鍵を用いて生成する。

## 【0039】

S209：サーバ機器100はクライアント機器101の機器識別子ID bに対応したPWを、パスワード記録部105から検索し、選択する。そしてクライアント機器101から送られた署名応答[B]を、選択したPWを用いて認証する。具体的にはr a、X bとPWを連結した情報、およびクライアント機器101の公開鍵を用いて、クライアント機器101の署名応答が正しいことを公開鍵暗号処理部104にて確認する。ここで認証が合わない場合は、PWあるいはクライアント機器101が正しいものではないと判断し、認証手続きを中止する。

## 【0040】

S210：クライアント機器101はサーバ機器100の署名応答[A]を同様に認証する。具体的にはr bとX aを連結した情報、およびサーバ機器100の公開鍵を用いて、サーバの機器100の署名応答[A]が正しいことを公開鍵暗号処理部110にて認証する。この認証が合わない場合は、サーバ機器100

が正しいものではないと判断し、認証手続きを中止する。

#### 【0041】

S211、S212：サーバ機器100およびクライアント機器101はそれぞれ、E C-DHの初期値を用いて、共通の認証鍵を計算する。

なお、このあとD T C Pでは、サーバ機器100からクライアント機器101に暗号化したコンテンツを配布してクライアント機器101においてこれを共通の認証鍵を用いて復号する。

#### 【0042】

なお、実施の形態1では機器間の認証は双方向、P Wの認証は片側（サーバ機器100がクライアント機器101のP Wを認証）であったが、これに限るものではなく、機器間の認証が片側、あるいはP Wの認証は双方であっても良い。P Wの認証で双方向にするとクライアント機器101が以前に自身がP Wを登録したサーバ機器100であるかを確認することができる。

#### 【0043】

##### 〔実施の形態2〕

実施の形態2では、実施の形態1におけるサーバ機器100のパスワード記録部105にユーザのパスワードを登録する機能を追加する。パスワードの認証は実施の形態1と同じである。

##### 〔実施の形態2の構成〕

図3は、実施の形態2における、サーバ機器100とクライアント機器101の内部構成を示している。

#### 【0044】

サーバ機器100は、実施の形態1におけるサーバ機器100に、パスワード入力部300と、入力されたパスワードが妥当であることをチェックするパスワードチェック部301と、さらにクライアント機器101と近くにあることを認証する近接認証部302を追加している。

一方、クライアント機器101は、実施の形態1におけるクライアント機器101に、サーバ機器100と近くにあることを証明する近接証明部303を追加している。サーバ機器100およびクライアント機器101のその他の構成要素

に関しては、図 1 と同じであるため、ここでは説明を省略する。

#### 【0045】

##### [実施の形態 2 のパスワード登録時動作]

実施の形態 2 におけるパスワードの登録には 2 通りある。1 つはサーバ機器 100 に直接入力する場合であり、もう 1 つは近接のクライアント機器 101 からのリモート入力の場合である。

サーバ機器 100 に直接入力する場合、入力されたパスワードはパスワードチェック部 301 において、妥当性をチェックしてからパスワード記録部 105 に記録される。妥当性のチェックでは、例えばパスワードの長さが十分であるかどうか、また辞書にある単語ではないか、またアルファベットだけではなく、数字や記号などの情報が含まれているかなどを確認する。

#### 【0046】

一方、リモート入力の場合、サーバ機器 100 とクライアント機器 101 の間で公開鍵暗号を用いた認証と鍵共有を行い、さらにサーバ機器 100 とクライアント機器 101 が近くにあるかどうかを確認することにより、クライアント機器 101 から入力されたパスワードがサーバ機器 100 に登録される。クライアント機器 101 からサーバ機器 100 に伝送されるパスワードは前記鍵共有した鍵を用いて暗号化してもよい。サーバ機器 100 とクライアント機器 101 が近くにあるかどうかの確認は、例えば次のような方法で行うとよい。

#### 【0047】

・IP パケットのヘッダにある TTL (Time To Live) フィールドを用いる。TTL はルータを越えるごとにデクリメントされるものである。例えばクライアント機器 101 の近接証明部 303 からある決められた TTL 値でサーバ機器 100 にパケットを送信し、サーバ機器 100 に到着したときの TTL 値との差分で、いくつルータを越えたのかを近接認証部 302 で調べることができる。この差分値が小さければ、サーバ機器 100 とクライアント機器 101 が近くにあると判断することができる。

#### 【0048】

・サーバ機器 100 の近接認証部 302 からクライアント機器 101 に Pin

g パケットを送信し、クライアント機器 101 の近接証明部 303 からの応答が返ってくるまでの時間をサーバ機器 100 の近接認証部 302 で測る。この値が小さければ、サーバ機器 100 とクライアント機器 101 が近くにあると判断することができる。

#### 【0049】

これにより、家庭内のクライアント機器 101 からのパスワード登録だけを受け付ける。

#### 〔実施の形態 3〕

実施の形態 3 では、サーバ機器 100 とクライアント機器 101 が近くにある場合と遠くにある場合で、有効となるパスワードを変更することを可能にする。クライアント機器 101 を家庭内で使用する場合は、簡略したパスワードを使用することによりユーザ利便性を確保し、リモートで使用する場合は長いパスワードを要求することにより、セキュリティを高めることが可能になる。

#### 【0050】

#### 〔実施の形態 3 の動作〕

実施の形態 3 の動作を、実施の形態 2 と同様の図 3 を用いて説明する。

パスワード記録部 105 には、家庭内で使用する場合はパスワードとリモートで使用する場合はパスワードを記録しておく。

サーバ機器 100 は、クライアント機器 101 の機器認証する際に、近接認証部 302 および近接証明部 303 を用いて、クライアント機器 101 が近くにあるのか遠くにあるのかを確認する。この方法としては、前述した実施の形態 1 と同様の TTL や Ping を用いるとよい。そして、その結果に応じてサーバ機器 100 はパスワード記録部 105 より、対応するパスワードを選択してパスワード認証時に使用する。パスワード認証は実施の形態 1 に従う。

#### 【0051】

なお、実施の形態 3 においては、家庭内とリモートの 2 種類のパスワードを使い分ける方法を述べたが、これを複数種類備えても良い。例えば TTL 値が 5 以下なら第 1 のパスワード、10 以下なら第 2 のパスワード、10 より大きいなら第 3 のパスワードといった具合である。これにより、例えば家庭内なら短いパス



ワードで利便性を向上し、（間のルータ数が少ない）専用線で接続されているオフィスとの間ではある程度の長さを確保したパスワードを利用し、（間のルータ数が多い）海外等の離れたところから利用する場合は、高度のセキュリティを備えたパスワードを利用することが可能となる。

#### 【0052】

なお、実施の形態1、2、3においては、IDに対応したパスワードを複数設けてもよい。もし1つのパスワードを忘れても覚えているパスワードを用いてサーバ機器100と認証できる。また、登録できるIDとパスワードを複数設けても良い。さらに、IDに対応して使用できるコンテンツを選択しても良い。例えば、家族のそれぞれで利用できるコンテンツを分けることができる。

#### 【0053】

また、実施の形態1、2、3におけるパスワード入力部は、一般的にはユーザがアルファベットや数字などをキーボードを用いて入力するが、携帯電話やリモコンのようなボタンを用いて入力しても良い。また、毎回は入力しなくてもよい。

また手で入力する替わりに、ICカードやセキュアメモリカードを用いても良い。

#### 【0054】

また指紋や虹彩などのバイオメトリックス情報を用いても良い。なお、バイオメトリックス情報は、入力時の誤りあるいは生体情報の多少の変動がありうる。この場合は、クライアント機器101においてデジタルデータであるパスワードを予め記録し、バイオメトリックスを用いて個人認証を行い、その結果本人であることが認証できた場合にのみ、クライアント機器101に記録しているパスワードを使用してパスワード認証を行っても良い。例えば実施の形態3では、リモート環境では、バイオメトリックス情報のみをPWとして使用可能とするといった使い方もできる。これにより、よりリモート環境でのセキュリティを高めることができる。

#### 【0055】

また、上記実施の形態1、2、3では、公開鍵暗号ベースのPW認証と機器認

証を説明したが、使用する暗号の種類は問わない。共通鍵暗号であっても、あるいは鍵を用いたハッシュ関数を用いても構わない。

#### 【0056】

##### 【発明の効果】

以上のように、請求項1に示した機器認証システムでは、機器認証だけでなく、機器に入力されたパスワードの認証を、そのトランザクションや計算量を増加せずに行うことができる。このことにより、勝手に接続されるというコンテンツ著作権保護の課題を解決する。

#### 【0057】

また、請求項4ではサーバと機器の間が近いのか離れているのかを判定する手段を加えることにより、リモートでのパスワードの登録を可能とする。

また、請求項6では請求項4と同様にサーバと機器の間が近いのか離れているのかを判定して、必要なパスワードを使い分ける。このことにより、例えば家庭内では簡易なパスワードを用いて利便性を確保し、リモート環境では長く複雑なパスワード、あるいはバイオメトリックス情報を用いて安全性を向上するといった使い方が可能となる。

##### 【図面の簡単な説明】

##### 【図1】

実施の形態1におけるサーバ機器とクライアント機器の内部構成図

##### 【図2】

実施の形態1のサーバとクライアント間の機器認証およびパスワード認証の動作フロー

##### 【図3】

実施の形態2におけるサーバ機器とクライアント機器の内部構成図

##### 【符号の説明】

100 サーバ機器

101 クライアント機器

102、109 秘密鍵格納部

103、108 公開鍵証明書格納部

1 0 4、1 1 0 公開鍵暗号処理部

1 0 5 パスワード記録部

1 0 6 認証部

1 0 7、1 1 3 入出力部

1 1 2、3 0 0 パスワード入力部

1 1 1 識別子格納部

3 0 1 パスワードチェック部

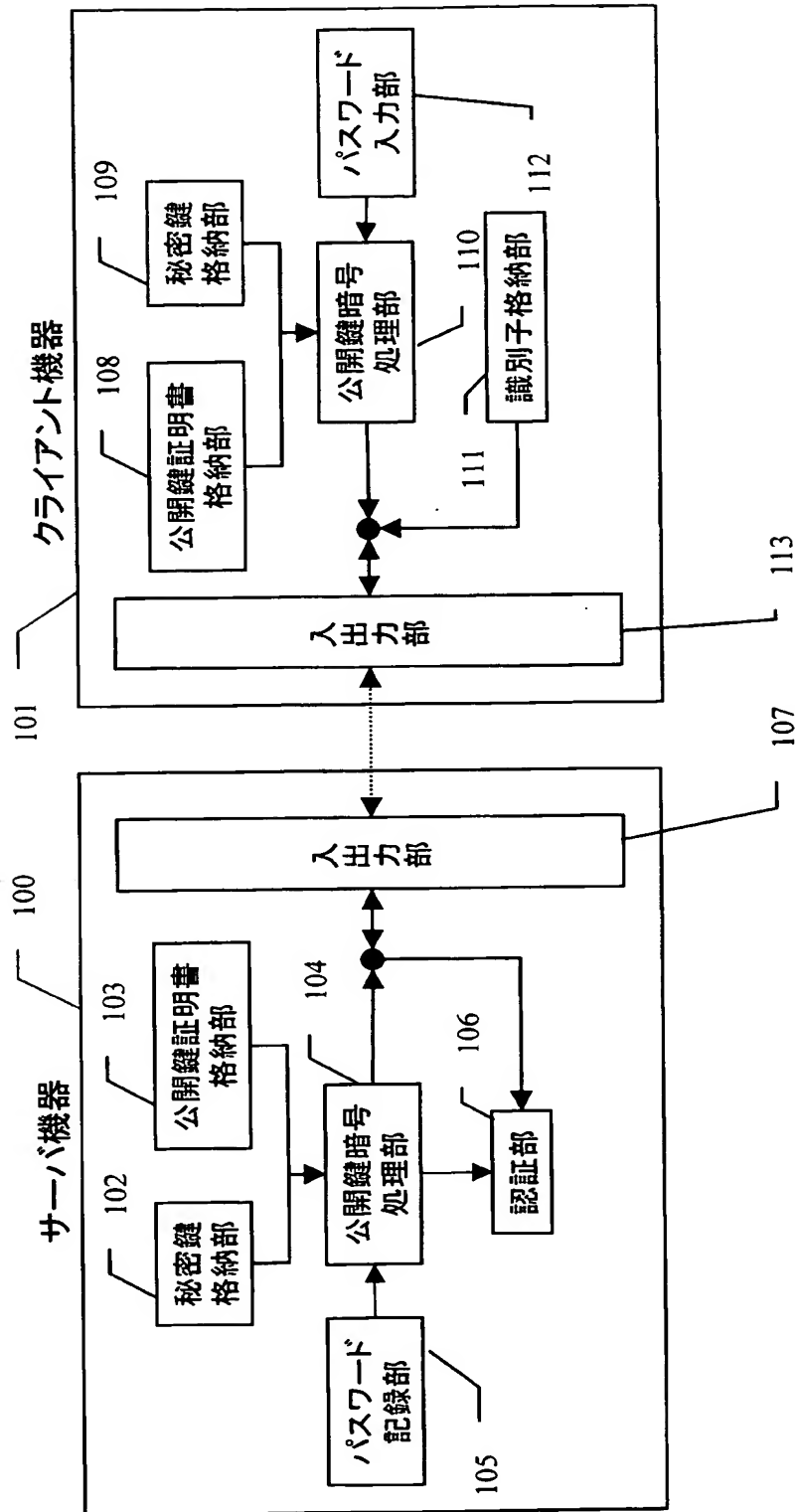
3 0 2 近接認証部

3 0 3 近接証明部

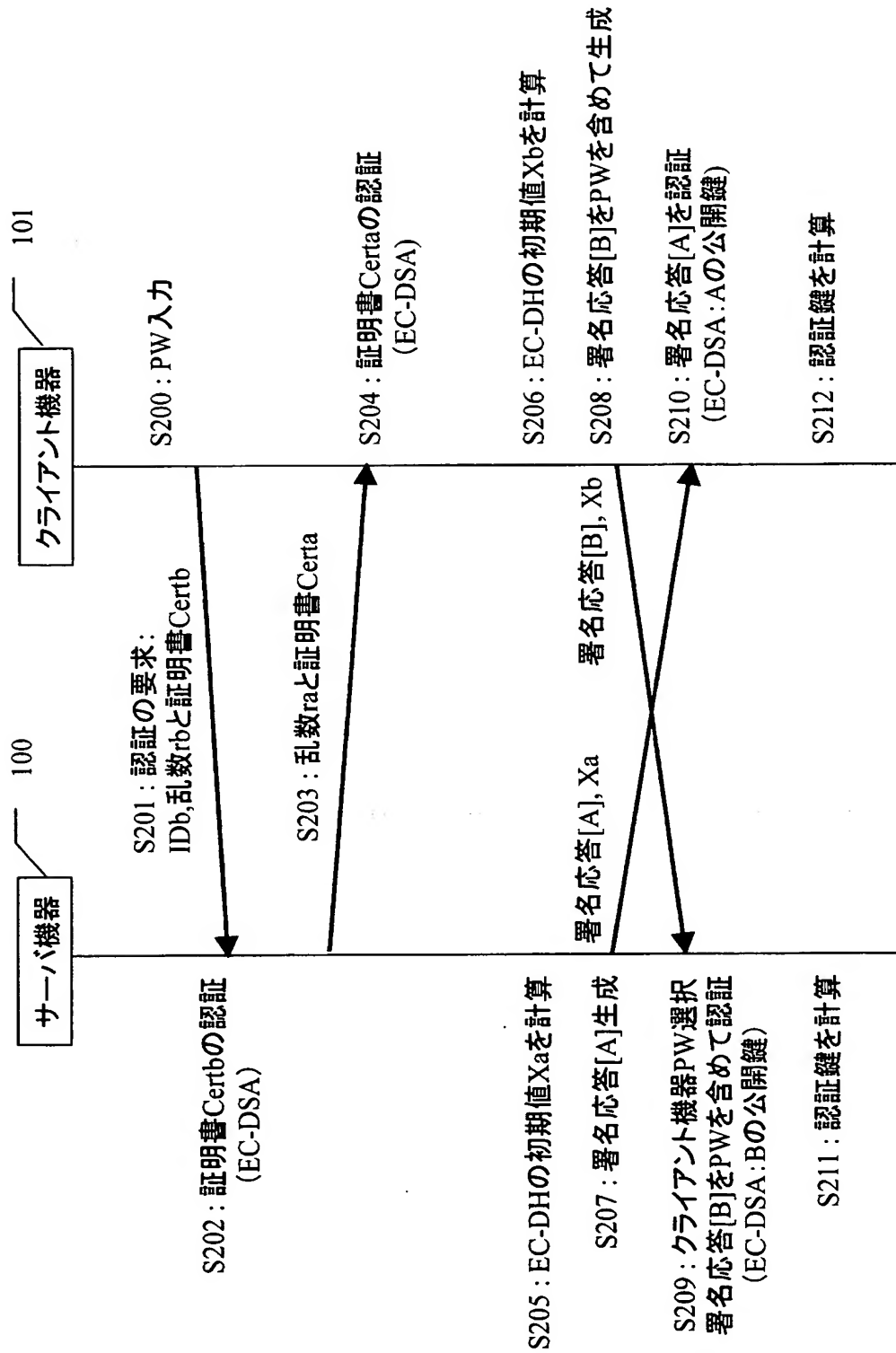
【書類名】

図面

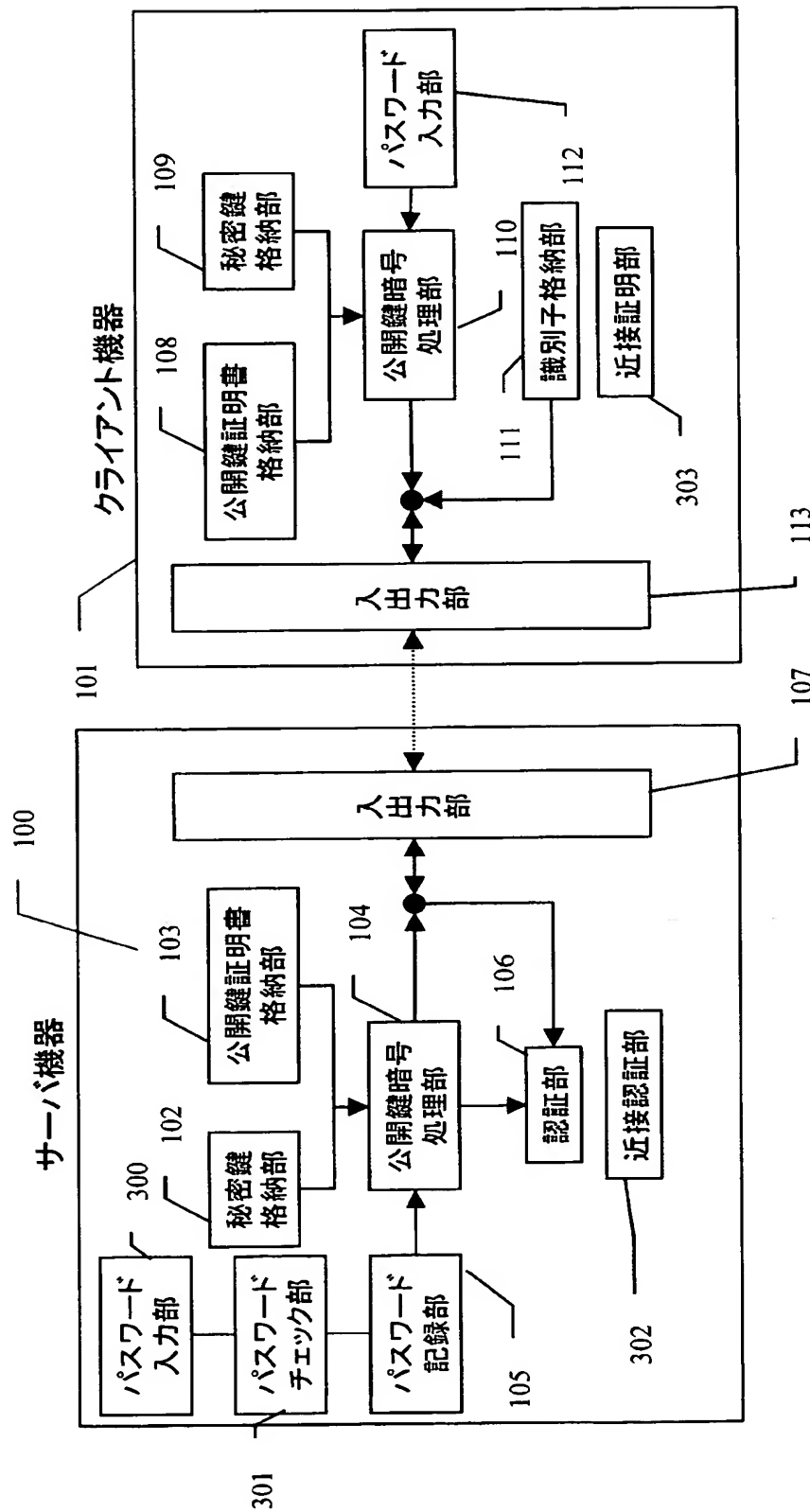
【図 1】



【図 2】



【図 3】



**【書類名】 要約書****【要約】**

**【課題】** コンテンツ保護の仕組みを無線通信の世界まで拡張したときに、コンテンツ保持者の許可がない機器が、勝手にサーバ機器に接続することを、実装上負荷をかけずに、防ぐことを目的とする。

**【解決方法】** 機器に入力されたパスワードを含めた署名を、チャレンジデータに対応したレスポンスとする。サーバ機器側は登録されているパスワードを含めてこれを認証することにより、トランザクションや計算量を増やさずに機器認証とパスワード認証を双方とも実現する。

**【選択図】 図 1**

特願 2 0 0 3 - 1 0 9 2 6 4

出 願 人 履 歴 情 報

識別番号 [ 0 0 0 0 0 5 8 2 1 ]

1. 変更年月日	1 9 9 0 年 8 月 2 8 日
[変更理由]	新規登録
住 所	大阪府門真市大字門真 1 0 0 6 番地
氏 名	松下電器産業株式会社